State of Montana
Office of the Legislative Auditor

REPORT ON REVIEW OF THE COMPUTER SERVICES FACILITY AND SELECTED APPLICATIONS

Each year, the Office of the Legislative Auditor reviews the central computer facility and selected computerized applications. This report provides information to auditors and agency management concerning the control strengths and weaknesses contained in the following:

- Computer Services Facility.
- Central Payroll System.
- Statewide Budgeting and Accounting System.
- Warrant Writing System.
- Property Accountability and Management System.

Office of the Legislative Auditor
Room 135, State Capitol
Helena, Montana 59620

83DP-13

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
HELENA, MONTANA 59620
406/449-3122

ROBERT R. RINGWOOD
LEGISLATIVE AUDITOR

DEPUTY LEGISLATIVE AUDITORS:
JAMES H. GILLETT
FINANCIAL/COMPLIANCE AUDITS
SCOTT A. SEACAT
PERFORMANCE AUDITS
STAFF LEGAL COUNSEL
JOHN W. NORTHEY

September 1983

The Legislative Audit Committee
of the Montana State Legislature

Herein transmitted is our central review of the Computer Services Division information processing center and selected automated applications. The purpose and scope of the review are explained in Chapter I of the report.

We wish to express our appreciation to the Director of the Department of Administration, the State Auditor and their staffs for their cooperation and assistance.

Respectfully submitted,

Scott A. Seacat
Deputy Legislative Auditor

Approved:

Robert R. Ringwood
Legislative Auditor

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

ADMINISTRATIVE OFFICIALS

DEPARTMENT OF ADMINISTRATION

Morris Brusett — Director

Accounting Division

Kathy Fabiano — Acting Administrator

Computer Services Division

Mike Trevor — Administrator

OFFICE OF THE STATE AUDITOR

E.V. "Sonny" Omholt — State Auditor

Central Payroll Division

Kathleen M. Behm — Administrator

Fiscal Management and Control Division

Josophie A. Isaak — Administrator

Chapter I

INTRODUCTION

This report results from our review of selected data processing operations of the state of Montana for the fiscal year ended June 30, 1983. Generally accepted governmental auditing standards require that both manual and data processing controls be considered when evaluating controls. This report informs auditors performing audits of state agencies or programs of controls within the centralized systems. In addition, the report informs agency managers of control strengths and weaknesses of the centralized systems. Agency managers may take appropriate steps to correct weaknesses, or design additional controls to compensate for weaknesses.

ORGANIZATION OF THE REPORT

This report is presented in six chapters. Chapter I presents an introduction to the report and summarizes the objectives and scope of our review.

Chapter II discusses centralized controls implemented over the CSD information processing facility (IPF). The information processing facility consists of the CSD computer center and support functions provided by CSD. IPF controls affect all users of the central information processing facility.

Chapter III discusses centralized controls within the central payroll portion of the Payroll, Personnel, and Position Control system. Chapters IV, V, and VI discuss centralized controls within the Statewide Budgeting and Accounting System (SBAS), Warrant Writing System, and the Property Accountability and Management System (PAMS).

OBJECTIVES OF THE REVIEW

The objectives of our review were to identify and evaluate the effectiveness of controls implemented for the CSD information processing facility and selected applications. We also performed compliance tests of key controls to ensure they were implemented as described.

SCOPE OF THE REVIEW

Our review of controls was conducted in accordance with generally accepted governmental auditing standards. We did not test compliance with all laws and regulations relating to the central information processing facility, or the selected applications. Nothing came to our attention that indicated non-compliance with laws and regulations we did not test.

During our review, we interviewed employees of the Department of Administration and the Office of the State Auditor to determine policies and procedures. We also examined documentation to supplement and confirm information determined through interviews.

Our review concentrated on centralized controls for the CSD information processing facility and the Central Payroll, SBAS, Warrant Writing, and PAMS applications. Control over the centralized operations mentioned above is largely supplemented by controls established within the operations of user agencies. We did not identify or review controls established by users of the centralized operations.

MANAGEMENT MEMORANDA

As a result of our review we issued management memoranda to the Department of Administration and the Office of the State Auditor.

The memorandum issued to the Department of Administration concerned findings related to disaster planning for both the central computer facility and the statewide budgeting and accounting system application, change controls over production programs, and usage of access control software.

The memorandum issued to the Office of the State Auditor concerned findings related to disaster backup for the central payroll and warrant writing systems.

Chapter II

INFORMATION PROCESSING FACILITY

The Department of Administration, Computer Services Division, operates a central Information Processing Facility (IPF) for state government. The IPF provides data processing services for use by state agencies. Processing is performed on an IBM 3033 Computer operating 24 hours a day except for times allocated for system maintenance.

A listing of system resources, along with a description of CSD standards, policies, and procedures is available in the CSD User Information Guide.

GENERAL CONTROLS

General controls are those controls which apply to the overall data processing environment. Our evaluation and testing of general controls included:

--Organization and Operation Controls

--Hardware and System Software Controls

--Physical Security

--Access Controls

--Data and Procedural Controls

We did not identify or review centralized system development controls. The Office of the Legislative Auditor will perform a separate audit of system development activities at the System Development Bureau (SDB) of the Computer Services Division. The SDB audit will include evaluation and compliance testing of system development controls.

ORGANIZATION CONTROLS

Organization controls ensure proper segregation of duties so that no one person has the ability to commit and conceal material errors or irregularities. Organization controls include:

--Segregation of functions between the Electronic Data Processing (EDP) department and users.

--General or specific authorization over the execution of transactions prohibiting the EDP department from initiating or authorizing transactions.

--Segregation of incompatable functions within the EDP department.

The Computer Services Division of the Department of Administration is organizationally independent from the users of the IPF. CSD is organized as a separate division of the Department of Administration.

Processing is initiated either directly by the user or by CSD under user authorization. A production work order is required prior to initiation of processing by CSD employees. Production work orders may give specific authorization to initiate processing or general authorization to process on a scheduled or as requested basis.

CSD also maintains internal segregation to ensure employees are not performing incompatible functions, such as system programming and application programming. The tape librarian function is included under the operations bureau. CSD uses a tape management system (TMS) which provides additional control over the tape librarian function. Access control software (see page 10) is used to prevent unauthorized access to system or applications programs by CSD employees.

HARDWARE AND SYSTEM SOFTWARE CONTROLS

Hardware and system software controls reduce the possibility of system failure due to hardware or software malfunctions.

Hardware is the physical equipment used for data processing. System software is the collection of programs that control the data processing activities. System software is often referred to as the operating system, or system control program. Hardware and system software controls include:

--Use of control features built into computer hardware and systems software.

--Controls over changes to hardware and systems software.

Most maintenance of CSD equipment is performed under a maintenance contract with the vendor. Under the maintenance contract, the vendor agrees to repair or replace malfunctioning equipment within a reasonable amount of time. As a part of maintenance contracts, vendors perform periodic inspections and maintenance of the central computer and other significant equipment items. Vendor maintenance contracts for significant equipment items also include a provision for limited business interruption liability in the event of equipment malfunction.

In addition to periodic maintenance, equipment malfunctions are recorded both manually by the computer operator on duty and automatically through the system software. CSD and vendor personnel review problem reports to identify equipment maintenance needs.

Hardware or system software problems reported by users are manually recorded by CSD employees. Significant and recurring

problems are assigned to appropriate CSD personnel, or reported to the vendor for correction. Changes made to hardware and system software are subject to the change control procedure described in the CSD User Information Guide.

Requests for changes are recorded on a CSD Change Request form. CSD management periodically reviews the change requests. Priorities are established and the change is assigned to appropriate CSD personnel. When a change is prepared, tested, and approved, a time is established for implementation.

A critical part of each hardware and system software change is the establishment of recovery or "fall back" procedures should a change fail, or have undesirable side effects. Recovery procedures for a majority of changes are to revert to the system configuration prior to the change.

Operating system changes are made using the IBM System Modification Program (SMP). Changes are logged, and concurrent changes are kept to a minimum. This assists CSD in relating any side effects to a particular system change.

PHYSICAL SECURITY

Physical security reduces the risk of accidental or intentional destruction of data and program files or equipment. Physical controls include:

--Physical safeguard of files, programs and documentation.

--Physical safeguard of the computer facility.

--A plan or method to ensure continuity of operations after major destruction of files or hardware breakdown.

We reviewed physical security controls at both the CSD computer center and the offsite storage vault. At both locations we found physical security was adequate.

The CSD computer center and offsite storage vault are both equipped with fire and smoke detectors. Temperature and humidity are controlled and closely monitored at both locations. The offsite vault is equipped with a burglar alarm for protection when the building is not staffed. The CSD computer center contains water detectors and sump pumps to guard against flooding.

Electricity to the center is conditioned to protect against power surges. A battery operated uninterruptable power supply is installed to provide continuous power during minor power outages, and to allow sufficient time for an orderly shutdown during a major power outage.

Disaster Recovery

Disaster Recovery procedures provide for the continuation of operation following a disaster. User agencies are primarily responsible for recovery of their applications following a disaster. CSD is responsible for recovery of the central computer center.

We reviewed the CSD disaster recovery plan and determined the plan was not operational during the audit period. An operational recovery plan is difficult to achieve. A timely recovery from a major disaster essentially requires a backup facility similar to the CSD computer center. Because of the numerous equipment and system software requirements, it is difficult to find a data center that is similar to CSD's.

We informed CSD of our findings relating to disaster recovery. CSD recognizes the weaknesses in the current plan. CSD management is currently evaluating various options for disaster recovery in the future.

One option being evaluated is the installation of a smaller but compatible system at another location in the capitol complex. This option is dependent on a state agency which is currently evaluating the purchase of computer equipment. If the equipment purchased is compatible with the CSD computer, it could provide some recovery capability for the state's critical applications.

We reviewed disaster backup for systems programs and critical system data files and determined backup was adequate. User agencies are responsible for the backup of application programs and data files. We did not review the adequacy of backup by user agencies.

ACCESS CONTROLS

Access controls prevent unauthorized access to system documentation, data and program files, and the computer equipment. Access controls include:

--Limit access to documentation to those persons requiring it in the performance of their duties.

--Limit access to programs and data files to persons authorized to process or maintain systems.

--Limit access to computer equipment to authorized individuals.

Physical Access

CSD has established policies for restricting access to CSD work areas. Doors to the computer room, tape library, and teleprocessing room are kept locked at all times. Unsupervised access

to these areas is restricted to authorized CSD employees. Access is available to other individuals and tour groups under the supervision of authorized CSD employees. Access to the offsite tape vault is limited to CSD management, shift supervisors, and tape handling personnel. CSD offices are locked during non-working hours.

Access to Data Files and Programs

Various facilities exist for protection of data and program files. CSD has recently installed a system called ACF2 which is discussed below. Prior to implementation of ACF2, passwords were primarily used to restrict access. The use of passwords was cumbersome both for users and CSD. As a result, most files were not protected from unauthorized access.

Other methods are also available for protecting files including authorization routines and physical removal of the files from the system. These methods are also very cumbersome and are for the most part unused.

Access Control Software

During the fiscal year 1982-83, CSD installed the ACF2 security software system. ACF is an acronym for Access Control Facility. ACF2 provides a convenient tool for restricting access to data on program files. Usage of computer resources such as terminals or storage devices can also be restricted.

ACF2 was first installed in December 1982 for testing. The system was first made available to protect agency data files in mid-April 1983. ACF2 protection is based on access rules written by each agency. A rule defines who may access the file and what

access is allowed (read the file, write on the file, etc.). If a file is protected, a rule must be written to allow access.

Each agency using the central computer system has assigned employees as agency security officers. Security officers are responsible for writing access rules to protect agency program and data files. Security officers also receive violation reports for their agency.

The ACF2 system was implemented to allow agencies to determine the level of protection provided over data files. The system can be set to one of three protection modes. LOG mode will log access violations, but will still allow access. WARN mode will warn the person attempting unauthorized access, and will log the violation. Access will still be allowed. Cancel (CNCL) mode will deny unauthorized access, notify the person attempting access, and log violations.

ACF2 was not implemented during the entire fiscal year. Many agencies were only beginning to write rules protecting data files as of June 30, 1983. ACF2 protection had not been established over use of the Customer Information Contral System (CICS), a telecommunications system used by many applications, and the Integrated Data Management System (IDMS), a data storage and retrieval system used by some applications. (CICS and IDMS are discussed in more detail on pages 13, 14 and 15.)

CSD has published a Data Security Guide and numerous ACF2 manuals are available which explain the ACF2 system in detail.

Production Program Library

CSD has established a central production program library. Production programs are programs that have been coded and tested

and are being used for processing. The purpose of a production program library is to provide control over authorized changes and prevent unauthorized changes to production programs. Access to this production library is restricted and program changes are controlled by the Production Services Section of the CSD Operations Bureau.

To change a program stored in the production library, a user must first prepare and test the change. The user then prepares and signs a CSD change request form indicating that the program has been tested. The Production Services Section supervisor then moves the program into the production library. A copy of the change request form is then returned to the user. CSD does not review the testing, or the changed code prior to placing a program into the production library.

During our review, we determined that CSD does not maintain a listing of owners of production library programs. There is also no listing of personnel authorized to change production programs for each agency. Distributing a copy of the change request form to the owning agency provides some compensating control to ensure unauthorized changes are detected. In addition, CSD employees are familiar personnel submitting changes to large applications in the production library.

DATA AND PROCEDURAL CONTROLS

Data and procedural controls provide a framework for controlling daily operations and establishing safeguards against processing errors. Data and procedural controls consist of:

--A control or balancing function.

--Review of data processing activities by internal auditors, or an independent control function.

--Written manuals in support of systems and procedures.

--Fallback procedures to restore or replace lost, damaged, or incorrect files.

Data and procedural controls for substantially all applications are performed by the user agency. We did not identify or review data and procedural controls performed by user agencies. CSD does not have internal auditors, or an independent control group which periodically reviews data processing activities.

The CSD operations bureau performs input and output control functions for a few of the larger applications. Procedures performed by CSD are performed under the general authorization of the agency controlling the application. A production work order is required before CSD will perform input or output (I/O) services. CSD performs I/O services in accordance with procedures developed, or approved by the user agency and documented in a system operations manual.

Our review of compliance with procedures was limited to procedures performed for the SBAS, Central Payroll, and Warrant Writing application described later in this report.

Customer Information Control System

The IBM Customer Information Control System (CICS) is used as a communication control system for many state applications. CICS facilitates entry, modification, and retrieval of data using video terminals. CICS also provides numerous control features, including identification of the user, automatic error recovery,

usage statistics, and security violation logging. Our review of CICS was limited to its use for correction of accounting transactions in the Statewide Budgeting and Accounting System.

CSD has established standards for the usage of CICS. These standards are detailed in Chapter 8 of the CSD users guide. Procedures for reporting attempted security violations are described in Chapter 4 of the CSD user guide. CSD standards restrict CICS programming to properly trained programmers. All CICS programs and program modifications are reviewed by Technical Systems Bureau personnel to preserve the integrity of the CICS system.

Control features within CICS can be used to adequately protect transactions processed through CICS. CICS does not provide protection to data files unless the application program provides for exclusive control of the file. Files not under exclusive control can be accessed unless protected through ACF2 or by some other means.

Integrated Data Management System

The Integrated Data Management System (IDMS) is used as a database management system by CSD. Data base management systems are programs that manage the collection, storage, modification, and retreival of data stored in a data base. A data base is a centralized collection of data where data items (elements) are logically connected.

Data base management systems reduce the need for redundant information and the need to reprogram applications when the characteristics of data change. Data base management systems also provide a convenient facility for controlling the sharing of data between agencies or applications.

The use of IDMS is controlled by the CSD Data Management Services Bureau. The bureau has established standards for data base design and the naming of data elements. IDMS standards are included in Chapter 9 of the CSD user guide.

IDMS provides numerous control features. Use of these features will vary for individual applications. A major control feature allows the bureau to control which users may read or update which portions of the database.

Chapter III

CENTRAL PAYROLL SYSTEM

The State Auditor's Office, Central Payroll Division, is responsible for the operation, maintenance, and control of the Central Payroll System for state government. The Central Payroll System processes payroll for all state agencies with the exception of university system units and vocational-technical centers.

All six university system units process their own payroll. Payroll warrants for Montana State University and the University of Montana are printed and distributed at those locations. The remainder of the university system units process multiple vendor transfer warrant claims through the Statewide Budgeting and Accounting System. State warrants are then printed for the amount of the employee net pay. The warrants are mailed directly to the employee. Payroll for the vocational-technical centers is processed and distributed by local school districts.

Our review was limited to payroll transactions processed through the Central Payroll System. We did not examine controls over payroll processing or distribution at university system units or vocational-technical centers.

Central payroll transactions are processed through the Payroll, Personnel Position Control (PPP) system. Our review was limited to the payroll portion of the system. We did not identify or test controls relating to the personnel or position control functions of the system.

The Central Payroll Division has published a PPP system users manual. The manual provides agencies with instructions on

the use of the PPP system. The manual contains examples of forms used to provide information to the system and reports produced by the system.

INPUT CONTROLS

Input controls ensure that data is accurately and completely transferred from its source to machine-readable format and transactions are authorized for processing. Input controls include:

--Accepting only properly authorized input for processing.

--Edit of input data for validity.

--Control of data conversion process.

--Control of the movement of data.

--Controls to ensure errors are corrected and items are resubmitted for processing.

Biweekly Prepayroll

Biweekly payroll information is input using the prepayroll report. The prepayroll report contains employee payroll data (hours, pay rates, etc.) from the previous pay period. The prepayroll is generated by the PPP system and is distributed to each agency. Agency payroll clerks make the necessary changes to the prepayroll to reflect current pay period information. If employee payroll information is the same as the previous pay period, no changes to the prepayroll are necessary.

Data entry of prepayroll changes for the Department of Highways are performed at the department. When data entry is completed, a magnetic tape is generated. The tape is merged with other agencies' payroll information for processing. We did not

examine controls implemented by the Department of Highways to ensure payroll transactions are authorized and properly entered for processing.

Updated prepayroll reports are submitted to Central Payroll Division for processing. Upon receipt, prepayroll reports are reviewed for proper agency authorization.

We determined that the authorized signature list for central payroll transactions was out of date. We noted that Central Payroll Division employees were aware of changes in authorized signers. In our review we found no exceptions when testing for authorized signatures. We suggested that Central Payroll Division confirm authorized signers every six months and maintain a current authorized signature list. Central Payroll Division has since confirmed authorized signers and updated the signature list.

Following authorization review, prepayroll reports are logged on a check sheet and are submitted to the Data Entry Section of the Computer Services Division.

Data entry personnel access an on-line (magnetic disk) file of the prepayroll information. Changes are entered and key verified; unchanged data is not.

After prepayrolls are key entered, they are returned to Central Payroll. Prepayrolls are then logged on the check sheet as key entered and filed. When the check sheet indicates that prepayrolls for all agencies and locations have been key entered, payroll transactions are processed through a batch balance and edit routine. Data is edited for validity and computer generated control totals for hours, rate, and gross pay are compared to

agency prepared totals which were input. Any transactions containing invalid data and any pay locations where computer generated control totals disagree with agency prepared control totals are listed on error reports.

We reviewed system edits and determined reasonable edits existed to detect invalid data. We did not examine edits to determine if they were properly functioning during the entire fiscal year.

Central Payroll employees contact agency personnel to obtain corrections for invalid data. Corrections are then entered and control total differences are resolved. Once corrections are entered, the rejected transactions and out-of-balance locations are again processed through the balance and edit routine. When all locations are balanced and invalid data is corrected, the payroll is ready for processing.

Because of the cost to process the edit update routine, occasionally payroll is processed before all out-of-balance conditions are corrected. When Central Payroll determines it is not cost effective to process an additional balance and edit run, the transactions that are out of balance are deleted. The agency for which the employee works is informed. The agency can correct the employee's pay using one of two methods. If the difference is small, the deleted transaction can be corrected and added to the next biweekly payroll. If the difference is large, or the employee requests immediate correction, the correct payroll amount is manually calculated. A claim is then processed to generate a state warrant for the net pay amount. The Central Payroll records are then adjusted to reflect the payment.

We determined that the above situation occurred three times during fiscal year 1982-83. In all cases, we determined the employee was properly reimbursed and payroll records were corrected. A listing of each situation has been placed in the agency file for the affected agencies.

Occasionally it is necessary for agencies to phone in changes to payroll information after the prepayroll has been submitted to Central Payroll Division. Central Payroll accepts the change over the phone and requests the person making the change to send a memo to document the change. We noted that the person phoning in the change and signing the memo was not always the person authorizing payroll transactions. This could allow a payroll clerk or other person to circumvent payroll authorization controls. We suggested that Central Payroll require that memorandum documenting phoned-in changes contain an authorized signature for the agency. Central Payroll has since changed their policies to implement this recommendation.

Payroll Status Changes

New employees and rehired employees are initially placed on the payroll system using a payroll status form. Payroll status forms are also used for changing employee payroll information. A payroll deduction form is used to enter or change employee deductions on the system.

Payroll status forms and payroll deduction forms are prepared by the agencies and submitted to Central Payroll for processing. Upon receipt, Central Payroll personnel review each document to ensure no apparent errors exist and that the documents are properly authorized.

Documents are then logged on a check sheet and submitted to the CSD Data Entry Section for entry. Documents are key entered and key verified and are returned to Central Payroll. Central Payroll employees log each returned batch on the check sheet. Documents are then filed.

We determined that centralized controls are adequate to ensure that information submitted on biweekly prepayrolls, payroll termination forms, payroll status forms, and payroll deduction forms is properly authorized and is accurately and completely input for processing.

Centralized controls over phoned-in changes to prepayroll reports were not adequate to ensure all phoned-in changes were properly authorized. As was noted earlier, procedures have been altered to correct this weakness.

PROCESSING CONTROLS

Processing controls provide assurance all transactions are processed as authorized. Processing controls include:

--Reconciliation of control totals produced in processing to input control totals.

--Controls preventing the processing of the wrong file and detecting errors in file manipulation.

--Limit or reasonableness checks within the program.

--Run-to-run controls to ensure the output from one step is properly input for the next.

The central payroll system uses control totals on gross pay amounts to ensure all input is processed and files are properly updated.

Control totals ensure that individual gross pay amounts are properly calculated. Control totals (foots) of gross pay by pay location are calculated by the central payroll application and agreed to the same control totals prepared by agencies on the biweekly prepayroll report.

We selected a random sample of payroll transactions and recalculated the following amounts:

--Gross pay

--Net pay

--Federal income tax withholding

--State income tax withholding

--FICA (both employee and state share)

--Retirement amount (both employee & state share)

--Workers' Compensation premium

We also tested for compliance with the federal minimum wage law and for agreement of payee and net pay from the calculate detail report to the payroll warrants. All calculations tested were accurate.

During the fiscal year 1982-83, the central payroll revolving fund was not adequately reconciled to ensure the liability for deductions, withholdings, and payroll taxes recorded on the central payroll system reconciles to the liability recorded on the Statewide Budgeting and Accounting System. Central Payroll employees record transfers to and payments from the central payroll revolving fund in a hand-kept ledger. Procedures for recording transfers and payments provide some assurance that agencies and vendors are properly paid for deductions, withholding, and payroll taxes.

OUTPUT CONTROLS

Output controls ensure accuracy, completeness and security of data following processing. Output controls include:

--Reconciliation of output control totals to input and processing control totals.

--Review of output for reasonableness and comparison to source transactions.

--Distribution of output only to authorized users.

The payroll system updates the PPP data base and produces printed payroll reports and payroll warrants. The system also generates magnetic tape files of payroll data for use by other agencies. Central Payroll Division uses gross pay for all agencies to ensure completeness and accuracy of printed reports. Central Payroll reconciles gross pay from the calculated detail report with gross pay for W-2 forms written to ensure W-2 forms are accurately written. We determined that W-2 forms were properly prepared and distributed in compliance with state and federal regulations.

Computer Services Division distributes payroll reports to Central Payroll. Warrants and the original warrant register go to the Fiscal Management and Control Division of the State Auditor's Office. The State Auditor's Office then distributes payroll warrants as described on page 35 of this report. Central Payroll Division distributes payroll reports and a copy of the warrant register to each agency.

We determined output controls were adequate to ensure hard-copy reports and warrants were accurately produced and properly distributed.

The payroll system creates magnetic tape files for use by other agencies. We did not examine controls over the creation of magnetic tape files.

AUDIT TRAIL

We determined that information maintained by the central payroll system is adequate to trace transactions from inception to final disposition and vice versa.

SYSTEM DOCUMENTATION

Our review of application documentation was limited to obtaining an understanding of the central payroll system. We determined that documentation was adequate.

PAYROLL ACCRUALS

One of the design features of the PPP system is the ability to process the payroll accrual at year end. Payroll accrual procedures are described in year-end cutoff memos (Management Memos 2-82-2 and 2-83-2). We determined that central processing of the payroll accrual was as described in year-end cutoff memos. We did not test the reasonableness of accrual amounts.

Chapter IV

STATEWIDE BUDGETING AND ACCOUNTING SYSTEM

The Department of Administration, Accounting Division, operates the Statewide Budgeting and Accounting System (SBAS). SBAS is a double entry system that provides financial information that can be used to review and control agency financial transactions.

All transactions are input under the authority of the Accounting Division. The SBAS System processed approximately 3.8 million transactions during fiscal year 1982-83.

INPUT CONTROLS

Accounting transactions are initiated by agency personnel. Agency accounting personnel code transactions on SBAS forms. The forms may be submitted directly to the Accounting Division for processing. Agencies may also process SBAS forms and generate a magnetic tape, or disk file of SBAS transactions to be transmitted to the SBAS system. We did not review individual agency procedures for coding SBAS forms, or preparing and transmitting SBAS transactions.

Hard Copy Input

Hard copy input must be submitted to the Accounting Division. Agencies may segregate hard copy documents into batches. The Accounting Division batches unbatched input documents, and logs batch control totals. The Data Entry Section of the Computer Services Division key-enters and key-verifies batches of documents.

Remote Job and Magnetic Tape Input

During fiscal year 1982-83 the six university system units, the Department of Social and Rehabilitation Services, and the Department of Highways submitted SBAS transactions via Remote Job Entry (computerized data transmitted over phone lines) or magnetic tape. Magnetic tape and remote job entry transactions are processed through a reformat program to convert the transmitted record into a format acceptable by SBAS. The reformat program produces a report of control totals which is distributed to the Accounting Division and the transmitting agency. The Accounting Division uses this report in its batch reconciliation process. Agencies also receive a copy of control totals which may be used to reconcile transactions transmitted to transactions received for processing. We did not review this reconciliation for individual agencies submitting remote job or magnetic tape transactions.

Daily Batch Reconciliation

Following each daily processing run, the Accounting Division reconciles control totals for all batches input to the control totals of documents processed and rejected by validity edits. Reconciliation controls are adequate to ensure all SBAS input data received by the Accounting Division are input for processing.

Validity Edits

Before transactions are allowed to enter the update cycle of processing, all transactions are edited by a validity edit routine. Documents containing invalid transactions are rejected and placed in an error suspense file. A rejected document report is printed identifying the errors. Validity edits minimize the number of invalid transactions processed.

Suspense File Corrections

Documents rejected and output to the suspense file are corrected using an on-line error correction program.

The rejected documents for most state agencies are corrected by the Accounting Division. The Accounting Division contacts agencies with rejected documents by telephone to obtain the correct entry. Occasionally the Accounting Division will enter corrections without contacting the agency initiating the transactions. The Accounting Division will not contact the agency for the following corrections if the correct entry is obvious:

--Incorrect subsidiary detail ledger number format.

--The + or - sign was omitted.

--Input agency was omitted.

Several state agencies have the ability to make on-line corrections to SBAS documents input by their agency. The on-line correction program allows agencies to access and correct only those documents input by their agency.

The on-line correction program prevents certain changes from being made by the Accounting Division or user agencies. The program will not allow agencies to change the input agency, delete a transaction line, or purge a document from the file. Agencies cannot change the amount on purchase orders, or collection reports. Agencies are not allowed to make any changes to a SBAS notice of appropriation (form 212) or notice of revenue estimate (form 214).

Neither user agencies nor the Accounting Division can make changes to form code, document number, record for agency, or any warrant creating line.

The entire contents of the rejected document suspense file (both corrected and uncorrected transactions) are re-input for each SBAS daily processing run. Data re-input from the suspense file is again processed through the SBAS validity edits. Corrected documents enter the processing cycle and documents not corrected or only partially corrected reject to the suspense file. All corrections submitted through the on-line correction facility are logged on a suspense file correction report. The report shows the rejected transactions as they were originally input, and as corrected. Each agency receives a copy of the suspense file correction report for transactions input by the agency.

PROCESSING CONTROLS

Run-to-run Totals

Run-to-run totals used in the SBAS daily processing ensure that transactions input are processed and properly update subsidiary control ledgers and responsibility center records.

Update Edits

Agencies occasionally submit expenditure transactions which cause negative cash or appropriation balances. The SBAS Daily Processing Program allows such transactions to process; however, an edit exists which prevents the creation of a warrant. The Accounting Division reviews the appropriation control ledger and the daily cash balance report each day and notes these situations. When the negative balances return to positive, the Accounting Division submits the held warrant source records for warrant creations.

OUTPUT CONTROLS

Balancing Controls

The SBAS Month-End Programs sort SBAS control ledgers into various formats for the generation of SBAS monthly reports. During month-end processing, the control ledgers for each accounting entity are balanced to the general ledger for that entity to ensure that the general ledger was properly updated.

Totals on responsibility center and reporting center reports are agreed to the totals of the responsibility center control ledgers used to create the reports. If the above totals are not in agreement, the error message * TOTALS DO NOT AGREE * is printed on the responsibility center or reporting center report. The Accounting Division also receives a report listing situations where totals do not agree.

Balancing controls are adequate to ensure the Accounting Division or the agency is notified when the general ledger, responsibility center reports, or reporting center reports disagree with subsidiary control ledgers.

Report Distribution

SBAS hard copy and microfiche reports are distributed by the Accounting Division. Controls were adequate to ensure a proper and timely distribution of both hard copy and microfiche reports.

AUDIT TRAIL

We determined the information maintained by the SBAS system is adequate to trace transactions from inception to final disposition and vice versa.

description of the cash elimination process. The criteria for usage of cash elimination control accounts was different from the criteria used for fiscal year-end 1981-82. The difference in the criteria will affect the consistency of control account usage between the two fiscal years.

Agencies were allowed to record cash transactions during the adjustment period except on transfer warrant claims and no-warrant transfers.

YEAR-END CLOSING

The closing of SBAS nominal and budgetary accounts is performed automatically in the SBAS closing program. We examined the closing process and found controls adequate to ensure that SBAS is properly closed.

TREASURY FUND STRUCTURE CONVERSION

Following closing of SBAS for fiscal year 1982-83, and opening of SBAS for fiscal year 1983-84, SBAS entity numbers were converted to a new treasury fund structure. If implemented as described, the procedures used should have ensured a complete and accurate conversion to the new fund structure. We did not test the conversion for individual entities to determine all entities were accurately converted.

After the conversion process was completed, the Accounting Division generated a set of general ledger and subsidiary detail ledger reports. These reports titled Conversion 84 contain the same balances as the Post Closing 83 reports presented in the new fund structure.

Chapter V

WARRANT WRITING SYSTEM

The warrant writing system controls the creation and distribution of most state warrants and the redemption of all state warrants. The system accounts for state warrants issued, outstanding and redeemed. Payroll warrants for Montana State University (MSU) and the University of Montana (UofM) are created and distributed by the universities. We did not examine controls over the creation and distribution of Payroll Warrants at MSU or UofM.

In addition to state warrants, treasury checks are written by the Department of Administration, Treasury Division and the Department of Labor and Industry, Employment Security Division. Several state agencies also have contingent revolving funds. Contingent revolving funds are checking accounts controlled by agencies to be used for emergency payments, or small expenditures. Contingent revolving fund checks may be automatically generated by a check writing system, or manually written. Treasury checks and contingent revolving fund checks are not a part of the state warrant writing system and were excluded from our review.

The operation of the warrant writing system is controlled by the State Auditor's Office and the Accounting and Treasury Divisions of the Department of Administration. The State Auditor's Office is primarily responsible for the system. The Accounting Division initiates the warrant writing function and reconciles the system to the Statewide Budgeting and Accounting System (SBAS). The Treasury Division controls warrant redemption.

INPUT CONTROLS

The Accounting Division initiates the writing of warrants by preparing a warrant authorization form. The warrant authorization form details the amount and approximate number of warrants to be written for each type (series). Copies of the warrant authorization form are sent to the State Auditor's Office and Computer Services Division.

Upon receipt of the warrant authorization form, the Computer Services Division requests blank warrant stock from the State Auditor's Office and initiates warrant processing.

Warrant information input into the warrant writing consists of warrant source records. Warrant source records may be the warrant source files created by the Statewide Budgeting and Accounting System or the Department of Social and Rehabilitation Services Client Data Base System. Records may also be submitted by magnetic tapes generated from other data processing systems (Fish, Wildlife and Parks special license refunds, Public Employees' and Teachers' Retirement Systems etc.). In addition, a small number of warrant source records are submitted on punched cards.

Authorization by the Department of Administration, Accounting Division, is required to write warrants before recording the accounting transaction on the Statewide Budgeting and Accounting System. Accounting Division employees maintain records, and followup to ensure accounting transactions are recorded for all warrants written.

When processing is initiated, the total dollar amount of warrants to be written is input into the warrant writing system.

This amount is used as a control total to ensure all warrant source records are input and processed by the system.

PROCESSING CONTROLS

Warrant Writing

When warrants are written, a corresponding warrant record is placed on the outstanding warrants file. University of Montana and Montana State University payroll warrants are merged onto the outstanding warrants file through a warrant edit and load program.

When the State Auditor's Office receives the warrants, office personnel agree the amount and payee of most all purpose warrants to the corresponding warrant transmittal or multiple vendor warrant list prepared by the applicable agency. Excluded from this review are multiple vendor warrants submitted on magnetic tape (Fish, Wildlife and Parks special license refunds, retirement system warrants, etc.). Agreement procedures for multiple vendor warrants with detail submitted on magnetic tape vary for each agency. We did not review procedures for each of the various systems.

Central payroll and all purpose warrants are sequence checked to ensure all warrants are sequentially numbered and no warrants are missing.

Warrant Redemption

The Treasury Division receives warrants and a magnetic tape of warrant records that have cleared the bank on a daily basis. Warrants are first agreed by warrant number and amount to the bank tape. Discrepancies are researched and corrected. Next, the bank tape is processed against the outstanding warrants file to

determine that the warrant is outstanding and has not been cancelled, voided, or a stop payment has not been issued. Warrants from the bank that match valid outstanding warrant records on the outstanding warrant file are coded by the system as cashed.

Month-end Processing

At each month-end the warrant records for cashed warrants, cancelled warrants and warrants voided by the State Auditor's Office are removed from the outstanding warrant file. Month-end reports are produced to show the status of warrants issued and to provide information for the monthly warrant reconciliation.

OUTPUT CONTROLS

Warrant Reconciliation

The Warrant Writing System produces reports to control the processing of the system. Following each daily warrant writing run, the Accounting Division reconciles warrants written to warrant transactions processed on the Statewide Budgeting and Accounting System (SBAS). The Accounting Division also performs a monthly reconciliation of the general warrant account to ensure warrant transactions processed reconcile to warrants issued.

At each calander month-end, the State Auditor's Office reconciles State Auditor records of outstanding warrants to amounts recorded on the outstanding warrant computer file and SBAS.

Warrant Distribution

Distribution of warrants produced by the warrant writing and central payroll systems is controlled by the State Auditor's Office. Warrants are either mailed directly to the recipient indicated on the warrant or picked up at the State Auditor's Office. In the

latter case, agency personnel must be authorized to receive warrants and must sign for the warrants received.

We determined output controls were adequate to ensure that the State Auditor's Office releases warrants only to authorized personnel and that output reports accurately reflect the results of processing.

AUDIT TRAIL

We determined that information maintained by the warrant writing system is adequate to trace transactions from inception to final disposition and vice versa.

SYSTEM DOCUMENTATION

Our review of application documentation was limited to obtaining an understanding of the warrant writing system. We determined that documentation was adequate.

Chapter VI

PROPERTY ACCOUNTABILITY AND MANAGEMENT SYSTEM

The Property Accountability and Management System (PAMS) is a subsystem of the Statewide Budgeting and Accounting System (SBAS). PAMS is used to account for fixed assets owned by state agencies.

During our preliminary review of the PAMS system, we determined that controls to ensure fixed asset information is properly entered on PAMS are largely the responsibility of user agencies. We also determined that use of the PAMS system is inconsistent from user to user.

A detailed description of the PAMS system, and statewide policies for property accounting are contained in chapter 1700 of the Montana Operations Manual.

Input Controls

PAMS documents are prepared by the user agency and submitted to the Accounting Division for processing. The Accounting Division retains documents until PAMS processing is to be initiated. Usually PAMS processing is performed monthly. PAMS forms are key entered and key verified by the Data Entry Section of the Computer Services Division. PAMS documents are then returned to the Accounting Division.

When PAMS processing is initiated, PAMS transactions are edited by a validity edit routine. Invalid transactions are deleted from processing, and are printed on an error report. When the Accounting Division receives error reports, the original PAMS document is attached to the error report. The documents and

error reports are returned to the submitting agencies. The Accounting Division disposes of PAMS documents that process properly.

PAMS documents are not batched and no control total reconciliation is performed to ensure all documents are properly input for processing. No log of rejected transactions is kept to ensure rejected transactions are corrected and reinput for processing.

Because of the above, agencies should have established procedures to ensure all PAMS documents submitted have been properly input and processed by the PAMS system.

Consistency

The various agencies have established several different policies for accounting for fixed asset items. Several agencies have continued to maintain fixed asset accounting systems that existed prior to PAMS. These agencies submit summary entries to PAMS for each class of property. Many agencies record property that is valued less than the established limit of $200. For the most part, item costing less than $200 that are recorded are small costly items that are subject to theft or loss (cameras, guns, etc). Some agencies group small items together and enter a single entry on PAMS (file cabinets, chairs, etc.).

Because of weaknesses noted in input controls and the inconsistent usage of PAMS, we decided not to continue our review of the system. It appears more appropriate to examine controls and policies for the PAMS system at each individual agency.